Amendments to the Specification:

Please replace the paragraph that begins on page 4, line 22, with the following paragraph:

Software produced this way will only run on the CPU that produced the original response C1. This allows one to protect against software piracy, in that a manufacturer can produce software that runs on only one CPU. (The scheme extends easily to handle the case that the user owns multiple CPUs, by embedding multiple ciphertexts in the software, and seeing if any of them compare successfully.) Note that manufacturers cannot get together off-line to compare what they know, since all they have are ciphertexts produced using unknown keys for plaintexts of which they only know half. There is no way to "link" together different results of the "challenge" instruction, without using the very same chip on which those results were produced. ~~(End of Professor Rivest's proposal.)~~

Please replace the paragraph that begins on page 10, line 5, with the following paragraph:

Part (ii) As in FIG. 3, the content receiver in FIG. 4 encrypts the RC and sends EC to the content provider ~~which~~. As an example, EC may include RN and CID.